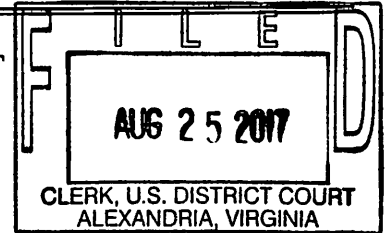


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Gray Apple Notebook Computer
Model: A1706
S/N: C02TK43JGTFJ

Case No. 1:17-SW-541

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Gray Apple Notebook Computer; Model: A1706, S/N: C02TK43JGTFJ, as described in Attachment A.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1)	Possession with Intent to Distribute a Controlled Substance;
21 U.S.C. § 846	Conspiracy to Distribute a Controlled Substance;
18 U.S.C. § 1956	Money Laundering.

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SAUSA Philip Trout/AUSA Samantha Bateman

Applicant's signature

Alexander G. Milne, Special Agent, IRS-CI

Printed name and title

Sworn to before me and signed in my presence.

Date: 25 Aug 17City and state: Alexandria, Virginia

/s/

Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

The property to be searched consists of computers hereinafter referred to as “the Devices.” The Devices, currently located at the Fairfax County Police Department Organized Crime and Narcotics Section in the Eastern District of Virginia, are:

1. BLACK ASUS LAPTOP COMPUTER, MODEL: 7260H, FCC ID: MSQ7260H, IC: 3568A-7260H, S/N: E7N0CJ012382289 (“Device 1”);
2. GRAY APPLE NOTEBOOK COMPUTER, MODEL: A1706, EMC: 3071, FCC ID: BCGA1706, IC: 579C-A1706, S/N: C02TK43JGTFJ (“Device 2”);
3. SILVER APPLE NOTEBOOK, MODEL: A1466, EMC: 2632, FCC ID: QDS-BRCM1072, IC: 4324A-BRCM1072, S/N: C02MQVT4GO85 (“Device 3”).
4. SILVER I-PHONE, MODEL A1688, FCC ID: BCG-E2946A, IC: 579C-E2946A (“Device 4”)
5. ROSE GOLD I-PHONE, MODEL A1688, FCC ID: BCG-E2946A, IC: 579C-E2946A (“Device 5”)

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

1. All records on the Devices described in Attachment A that relate to violations of 21 U.S.C. § 841, 21 U.S.C. § 846, 18 U.S.C. § 1956, 26 U.S.C. § 7201, and 26 U.S.C. § 7203, including, but not limited to:

a. Records and information relating to or showing a relationship between or among John KESTEL and other co-conspirators, to include those who purchased illegal drugs from John KESTEL;

b. Records and information relating to personal and business finances and financial transactions, including but not limited to: invoices, cash, paystubs, wages, bank statements, checks, check registers, check stubs, wire transfers, deposit slips, mortgages, deeds, rental contracts, and insurance;

c. Documents related to or memorializing the ordering, purchasing, storage, transportation and sale of controlled substances, including U.S. currency used in the purchase and sale of controlled substances, buyer lists, seller lists, pay-owe sheets and records of sales, log books, drug ledgers, personal telephone/address books of customers and suppliers, records relating to domestic and foreign travel such as tickets, passports, visas, credit card receipts, travel schedules, receipts and records, trucker log books and storage records, such as storage locker receipts and safety deposit box rental records.

d. Records and information relating to banks and financial institutions, including but not limited to: bank statements, passbooks, deposit or withdrawal slips, canceled checks, bank receipts, bank checks, money orders, loan documents, mortgages, safe deposit box keys, credit cards, charge receipts, investment accounts, and retirement accounts;

e. Records and information relating to taxes and tax liabilities, including but not limited to: tax forms (including IRS Forms 1099, 1040, and W-2), tax returns and schedules, IRS publications, correspondence to and from the IRS, IRS website access, income, dependents, receipts, expenses, deductions, credits, assets, liabilities, tax payments and refunds;

f. Records and information relating to employment, including but not limited to: job applications, resumes, references, fringe benefits, and correspondence;

g. Records and information relating to or used to record, store, or retrieve names, addresses, telephone numbers, and messages;

h. Records and information relating to the use of the U.S. Postal Service or commercial carriers, including any U.S. Postal Service or similar depository access keys;

i. Records and information relating to storage facilities, including but not limited to rental agreements, contracts, access codes and any keys to storage lockers or other storage-type facilities;

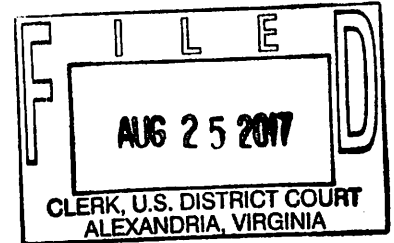
j. Photographs of participants and fruits and evidence of the trafficking of controlled substances.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records of or information about any routers, modems, and network equipment used to connect the Devices to the Internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The terms “electronic storage media” and “digital devices” include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF:)	<u>FILED UNDER SEAL</u>
)	
BLACK ASUS LAPTOP COMPUTER)	
MODEL: 7260HMY)	
FCC ID: MSQ7260H)	
IC: 3568A-7260H)	
S/N: E7N0CJ012382289)	<u>(UNDER SEAL)</u>
)	
GRAY APPLE NOTEBOOK COMPUTER)	
MODEL: A1706)	No. 1:17-SW-540
EMC: 3071)	
FCC ID: BCGA1706)	
IC: 579C-A1706)	No. 1:17-SW-541
S/N: C02TK43JGTFJ)	
)	
SILVER APPLE NOTEBOOK)	No. 1:17-SW-542
MODEL: A1466)	
EMC: 2632)	
FCC ID: QDS-BRCM1072)	No. 1:17-SW-543
IC: 4324A-BRCM1072)	
S/N: C02MQVT4GO85)	No. 1:17-SW-544
)	
SILVER I-PHONE MODEL A1688)	
FCC ID: BCG-E2946A)	
IC: 579C-E2946A)	
)	
ROSE GOLD I-PHONE MODEL A1688)	
FCC ID: BCG-E2946A)	
IC: 579C-E2946A)	
)	
CURRENTLY LOCATED AT)	
Fairfax County Police Department)	
Organized Crime and Narcotics Section)	

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Special Agent Alexander Gregory Milne, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent employed by Internal Revenue Service, Criminal Investigation ("IRS-CI") in the Washington, D.C. field office. I have been employed with IRS-CI since September 2011. My responsibilities include the investigation of possible criminal violations of the Internal Revenue laws under Title 26 of the U.S. Code and related offenses, particularly as found in Title 18 and Title 31 of the U.S. Code. I have several years of education, training, and experience in the fields of accounting, finance, tax, and criminal investigations. I earned a Bachelor of Business Administration Degree in Management and Organizational Behavior in May 2008. I graduated from the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in December 2011 and from Special Agent Basic Training at the National Criminal Investigation Training Academy in March 2012. In addition to my nearly five years of experience as a criminal investigator for IRS-CI, I have one and a half years of work experience as an auditor at the Department of the Treasury, Office of the Inspector General. My training and experience have provided me with a working knowledge of finance, accounting, tax law, and criminal investigations. My law enforcement training has included instruction on financial and criminal investigative techniques, as well as tax and criminal law, which includes the identification and development of probable cause to support the execution of arrest, search, and seizure warrants.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

3. Based upon the facts set forth herein, I submit there is probable cause to believe that John KESTEL (hereinafter “KESTEL”), Angie WIESE (hereinafter “WIESE”) and Thomas FROST (hereinafter “FROST”) have knowingly and unlawfully possessed with the intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(a)(1) and 846, and knowingly conducted a financial transaction affecting interstate commerce that involved specified unlawful activity to conceal or disguise the source or control of the proceeds of the unlawful activity, in violation of Title 18, United States Code, Section 1956. I further submit that there is probable cause to believe that KESTEL willfully attempted to evade taxes, in violation of Title 26, United States Code, Section 7201, and willfully failed to file a tax return, in violation of Title 26, United States Code, Section 7203. I further submit that there is probable cause to believe that the devices described in Attachment A contain evidence of these offenses.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched consists of computers and cellular phones (hereinafter collectively referred to as “the Devices”). The Devices are currently located in an evidence locker located at the Fairfax County Police Department Organized Crime and Narcotics Section, within in the Eastern District of Virginia. The Devices are:

- a. BLACK ASUS LAPTOP COMPUTER, MODEL: 7260HMY, FCC ID: MSQ7260H, IC: 3568A-7260H, S/N: E7N0CJ012382289 (“Device 1”);
- b. GRAY APPLE NOTEBOOK COMPUTER, MODEL: A1706, EMC: 3071, FCC ID: BCGA1706, IC: 579C-A1706, S/N: C02TK43JGTFJ (“Device 2”);
- c. SILVER APPLE NOTEBOOK, MODEL: A1466, EMC: 2632, FCC ID: QDS-BRCM1072, IC: 4324A-BRCM1072, S/N: C02MQVT4GO85 (“Device 3”);
- d. SILVER I-PHONE, MODEL A1688, FCC ID: BCG-E2946A, IC: 579C-E2946A (“Device 4”)
- e. ROSE GOLD I-PHONE, MODEL A1688, FCC ID: BCG-E2946A, IC: 579C-E2946A (“Device 5”)

5. The applied-for warrants would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. At all times relevant herein, IRS-CI, the Drug Enforcement Administration, and other federal and local agencies are investigating a network of individuals who are believed to have been manufacturing and selling anabolic steroids, which are Schedule III controlled substances.

7. The co-conspirators are believed to have been using the Internet and other means to advertise and sell the anabolic steroids they manufactured to various people across the United

States and other countries. The co-conspirators would receive payment for the anabolic steroids they sold through Internet-based financial institutions and would mail the anabolic steroids through the United States Postal Service.

8. The investigation, including evidence obtained through the execution of other search warrants, has revealed that the co-conspirators in this steroid scheme have used electronic means to communicate, receive orders, track orders, create invoices for orders, receive payments, and transfer funds from online financial institutions. Co-conspirators have used cellular phones to text order information to purchasers. Records provided by online financial institutions have shown that co-conspirators have conducted transactions through computers and mobile devices.

9. Based on my knowledge, training, and experience, individuals who engage in the above-described type of criminal activity may use desktop computers, laptop computers, notebooks, and tablet computers, personal digital assistants, wireless communication devices (such as cellular telephones and smart phones), or other electronic devices, to communicate with co-conspirators and to store documents and records relating to their illegal activity. Criminals store these documents and records on electronic devices, which can include contact information of co-conspirators, customer order information, addresses where illegal items were shipped, and records of transactions.

10. As set forth below, KESTEL and others are believed to be co-conspirators in the above-described scheme. It is believed that KESTEL manufactured anabolic steroids at his residence. KESTEL and others would receive orders from various individuals through text messages, email, and online marketplaces. WIESE received shipments believed to be in

furtherance of the conspiracy. This includes shipments addressed to WIESE containing stainless steel parts suspected of being used as replacement components for tablet presses, as well as shipments addressed to WIESE suspected of containing microcrystalline cellulose, a binding agent used in the manufacture of pills and capsules. Meanwhile, FROST participated in the conspiracy by, among other things, sending payments to China by wire to purchase chemicals used in the manufacture of the controlled substances.

11. On June 14, 2017, officers of the Fairfax County Police Department ("FCPD"), Organized Crime and Narcotics Section were serving an arrest warrant on FROST at 7903 Bethelen Woods Lane, Springfield, Virginia 22153. WIESE (aka Angie Wiese Verastegui), who is KESTEL's wife, was at the residence and stated that FROST no longer lived at the residence. WIESE gave the officers consent to enter the residence. While searching for FROST and clearing the basement of the residence, officers observed an unknown amount of a green leafy substance believed to be marijuana in plain view on the coffee table.

12. On June 14, 2017, Detective J. Rhoads, who is assigned to the FCPD Organized Crime and Narcotics Section, secured a search warrant from the Fairfax County Circuit Court for the premises located at 7903 Bethelen Woods Lane, Springfield, VA 22153, which is located in the Eastern District of Virginia.

13. On June 14, 2017, FCPD Officers, pursuant to the search warrant issued June 14, 2017, searched the premises located at 7903 Bethelen Woods Lane, Springfield, VA 22153. During the search, officers seized various drug evidence, drug manufacturing paraphernalia, paper documents, and the Devices described in Attachment A.

14. Some of the drug evidence that FCPD seized included the following:
 - a. Approximately three kilograms of a substance labeled “Test Prop,” which is believed to be Testosterone Propionate, a Schedule III controlled substance.
 - b. Approximately four kilograms of a substance labeled “Test E,” which is believed to be Testosterone Enanthate, a Schedule III controlled substance.
 - c. Approximately two kilograms of a substance labeled “Test Cyp,” which is believed to be Testosterone Cypionate, a Schedule III controlled substance.
 - d. Approximately one kilogram of a substance labeled “Primo Ace,” which is believed to be Methenolone Acetate, a Schedule III controlled substance.
15. The FCPD also seized drug manufacturing and distribution paraphernalia, including:
 - a. An Antramatix DP-1.5 single tablet press machine with production capacity of 5000 PCS (S/N 150702).
 - b. Tablet press machine replacement parts.
 - c. A pump, a heating device, and sterilizers.
 - d. Packaging supplies for liquid steroids and plastic packets for tablets.
 - e. Labeling supplies.
16. The documents that FCPD seized included the following:

- a. Electronically generated invoices from “Alpha Labs” listing various customers and their addresses, the various drugs requested, the total price of those drugs, the total price of the order, and hand written notes regarding the shipment of the various drugs.
- b. Copies of text messages received on a mobile device from various customers requesting specific quantities of drugs offered by KESTEL and hand written notations on the copies.
- c. Copies of email messages received from an online ordering system detailing the orders place by customers such as the type and amount of drugs requested and hand written notations.
- d. Wire transfer requests from Wells Fargo documenting payments from FROST to individuals in China suspected of being the source of supply for the steroids and illegal substances.
- e. Articles of Incorporation for the state of Virginia for Titan Labz, LLC.
- f. A CP 575A Notice from the Internal Revenue Service (“IRS”) to Titan Labz LLC, Alpha Research, John Russell Kestel Sole Mbr at 7903 Bethelen Woods Lane, Springfield, VA 22153, providing an Employer Identification Number to John KESTEL for Titan Labz LLC Alpha Research.

17. The FCPD found passports for KESTEL and WIESE in a closet of the master bedroom of the residence. They also found an assault rifle in a closet of the master bedroom of the residence.

18. The FCPD seized the Devices from the following locations inside the residence:

- a. Device 1 was located in the basement in the same room as the drug evidence described above.
- b. Device 2 was located in the upstairs master bedroom.
- c. Device 3 was located in the main floor living room.
- d. Device 4 was located in the upstairs master bedroom.
- e. Device 5 was located in a purse believed to belong to WIESE, who is believed to be the only adult female living in the residence.

19. Records received from an online financial institution showed that KESTEL provided the residential address of 7903 Bethelen Woods Lane, Springfield, VA 22153 as the address of Titan Labz. Law enforcement databases also show that KESTEL is a resident of 7903 Bethelen Woods Lane, Springfield, VA 22153. WIESE told FCPD officers that she and KESTEL, her husband, lived at the address.

20. Internal Revenue Service ("IRS") records show the following:

- a. That for Tax Years 2014 and 2015, KESTEL did not file a Form 1040, Individual Income Tax Return.
- b. In Tax Year 2014, KESTEL earned wages of at least \$43,000 from an employer located in the District of Columbia.

- c. In tax year 2015, KESTEL earned wages of at least \$64,000 from an employer located in the District of Columbia, and had numerous stock transactions reported on Form 1099-B, Proceeds from Broker and Barter Exchange Transactions.

21. The Devices have been in the possession of the FCPD since their seizure as detailed in the paragraphs above. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of the FCPD.

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: An Internet Protocol address (or “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Modem: A modem translates signals for physical transmission to and from the Internet Service Provider, which then sends and receives the information to and from other computers connected to the Internet.
- d. Router: A router often serves as a wireless access point and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. The router is in turn typically connected to a modem.
- e. Cellular telephone: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless

telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

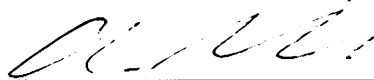
25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises.

CONCLUSION

27. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Alexander G. Milne
Special Agent
Internal Revenue Service- CI

Subscribed and sworn to before me
On August 25, 2017:



/s/

Ivan D. Davis

United States Magistrate Judge

ATTACHMENT A

The property to be searched consists of computers hereinafter referred to as “the Devices.” The Devices, currently located at the Fairfax County Police Department Organized Crime and Narcotics Section in the Eastern District of Virginia, are:

1. BLACK ASUS LAPTOP COMPUTER, MODEL: 7260HMY, FCC ID: MSQ7260H, IC: 3568A-7260H, S/N: E7N0CJ012382289 (“Device 1”);
2. GRAY APPLE NOTEBOOK COMPUTER, MODEL: A1706, EMC: 3071, FCC ID: BCGA1706, IC: 579C-A1706, S/N: C02TK43JGTFJ (“Device 2”);
3. SILVER APPLE NOTEBOOK, MODEL: A1466, EMC: 2632, FCC ID: QDS-BRCM1072, IC: 4324A-BRCM1072, S/N: C02MQVT4GO85 (“Device 3”).
4. SILVER I-PHONE, MODEL A1688, FCC ID: BCG-E2946A, IC: 579C-E2946A (“Device 4”)
5. ROSE GOLD I-PHONE, MODEL A1688, FCC ID: BCG-E2946A, IC: 579C-E2946A (“Device 5”)

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

1. All records on the Devices described in Attachment A that relate to violations of 21 U.S.C. § 841, 21 U.S.C. § 846, 18 U.S.C. § 1956, 26 U.S.C. § 7201, and 26 U.S.C. § 7203, including, but not limited to:

a. Records and information relating to or showing a relationship between or among John KESTEL and other co-conspirators, to include those who purchased illegal drugs from John KESTEL;

b. Records and information relating to personal and business finances and financial transactions, including but not limited to: invoices, cash, paystubs, wages, bank statements, checks, check registers, check stubs, wire transfers, deposit slips, mortgages, deeds, rental contracts, and insurance;

c. Documents related to or memorializing the ordering, purchasing, storage, transportation and sale of controlled substances, including U.S. currency used in the purchase and sale of controlled substances, buyer lists, seller lists, pay-owe sheets and records of sales, log books, drug ledgers, personal telephone/address books of customers and suppliers, records relating to domestic and foreign travel such as tickets, passports, visas, credit card receipts, travel schedules, receipts and records, trucker log books and storage records, such as storage locker receipts and safety deposit box rental records.

d. Records and information relating to banks and financial institutions, including but not limited to: bank statements, passbooks, deposit or withdrawal slips, canceled checks, bank receipts, bank checks, money orders, loan documents, mortgages, safe deposit box keys, credit cards, charge receipts, investment accounts, and retirement accounts;

e. Records and information relating to taxes and tax liabilities, including but not limited to: tax forms (including IRS Forms 1099, 1040, and W-2), tax returns and schedules, IRS publications, correspondence to and from the IRS, IRS website access, income, dependents, receipts, expenses, deductions, credits, assets, liabilities, tax payments and refunds;

f. Records and information relating to employment, including but not limited to: job applications, resumes, references, fringe benefits, and correspondence;

g. Records and information relating to or used to record, store, or retrieve names, addresses, telephone numbers, and messages;

h. Records and information relating to the use of the U.S. Postal Service or commercial carriers, including any U.S. Postal Service or similar depository access keys;

i. Records and information relating to storage facilities, including but not limited to rental agreements, contracts, access codes and any keys to storage lockers or other storage-type facilities;

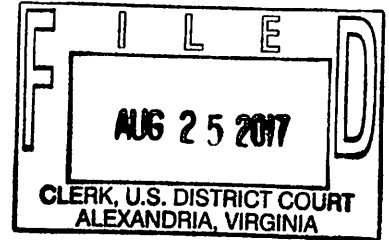
j. Photographs of participants and fruits and evidence of the trafficking of controlled substances.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records of or information about any routers, modems, and network equipment used to connect the Devices to the Internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The terms “electronic storage media” and “digital devices” include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF:)	<u>FILED UNDER SEAL</u>
)	
BLACK ASUS LAPTOP COMPUTER)	
MODEL: 7260HMY)	
FCC ID: MSQ7260H)	
IC: 3568A-7260H)	
S/N: E7N0CJ012382289)	<u>(UNDER SEAL)</u>
)	
GRAY APPLE NOTEBOOK COMPUTER)	
MODEL: A1706)	No. 1:17-SW-540
EMC: 3071)	
FCC ID: BCGA1706)	
IC: 579C-A1706)	No. 1:17-SW-541
S/N: C02TK43JGTFJ)	
)	
SILVER APPLE NOTEBOOK)	No. 1:17-SW-542
MODEL: A1466)	
EMC: 2632)	
FCC ID: QDS-BRCM1072)	No. 1:17-SW-543
IC: 4324A-BRCM1072)	
S/N: C02MQVT4GO85)	No. 1:17-SW-544
)	
SILVER I-PHONE MODEL A1688)	
FCC ID: BCG-E2946A)	
IC: 579C-E2946A)	
)	
ROSE GOLD I-PHONE MODEL A1688)	
FCC ID: BCG-E2946A)	
IC: 579C-E2946A)	
)	
CURRENTLY LOCATED AT)	
Fairfax County Police Department)	
Organized Crime and Narcotics Section)	

GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT
PURSUANT TO LOCAL RULE 49(B)

Upon the return of its executed search warrant,¹ the United States, by and through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the search warrant, application for the search warrant, affidavit in support of the search warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the search warrant and affidavit.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. At the present time, special agents of the Drug Enforcement Administration (DEA) and Internal Revenue Service, Criminal Investigation (IRS-CI) are conducting an investigation of a conspiracy to distribute controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846, money laundering, in violation of 18 U.S.C. § 1956, tax evasion, in violation of 26 U.S.C. § 7201, and failure to file a tax return, in violation of 26 U.S.C. § 7203.

2. Premature disclosure of the specific details of this ongoing investigation (as reflected, for example, in the affidavit in support of the search warrant) would jeopardize the investigation by revealing non-public information that could cause criminal targets to flee prosecution, destroy or tamper with evidence, or intimidate potential witnesses. A sealing order is therefore necessary to avoid hindering the continuing investigation.

¹ Pursuant to Local Rule 49(B), “[n]o separate motion to seal is necessary to seal a search warrant *from the time of issuance to the time the executed warrant is returned.*” (Emphasis added). This is because, as Rule 49(B) additionally mandates, “[u]ntil an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996). Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual

findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

5. However, regarding the notice requirement in the specific context of a search warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, in the context of search warrants, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government’s motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit’s precedents state that, “‘in entering a sealing order, a ‘judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,’” Media

General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate “decision to seal the papers” is “made by the judicial officer,” Goetz, 886 F.2d at 65. “Moreover, if appropriate, the government’s submission and the [judicial] officer’s reason for sealing the documents can be filed under seal.” Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) (“if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal”).

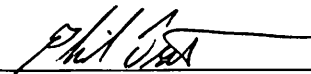
PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL
(See Local Rule 49(B)(3))

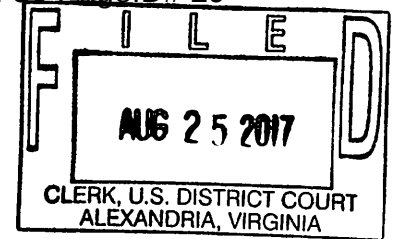
9. Pursuant to Local Rule 49(B)(3), the search warrant and the affidavit will remain sealed until the need to maintain the confidentiality of the search warrant application and the related investigation expires, after which time the United States will move to unseal the search warrant and affidavit. WHEREFORE, the United States respectfully requests that the search warrant, application for search warrant, affidavit in support of the search warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court.

Respectfully submitted,

Dana J. Boente
United States Attorney

By:


Philip Trout
Special Assistant United States Attorney



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF:)	<u>FILED UNDER SEAL</u>
)	
BLACK ASUS LAPTOP COMPUTER)	
MODEL: 7260HMY)	
FCC ID: MSQ7260H IC: 3568A-7260H)	
S/N: E7N0CJ012382289)	<u>(UNDER SEAL)</u>
)	
GRAY APPLE NOTEBOOK COMPUTER)	
MODEL: A1706 EMC: 3071)	No. 1:17-SW-540
FCC ID: BCGA1706 IC: 579C-A1706)	
S/N: C02TK43JGTFJ)	No. 1:17-SW-541
)	
SILVER APPLE NOTEBOOK)	No. 1:17-SW-542
MODEL: A1466 EMC: 2632)	
FCC ID: QDS-BRCM1072)	No. 1:17-SW-543
IC: 4324A-BRCM1072)	
S/N: C02MQVT4GO85)	No. 1:17-SW-544
)	
SILVER I-PHONE MODEL A1688)	
FCC ID: BCG-E2946A)	
IC: 579C-E2946A)	
)	
ROSE GOLD I-PHONE MODEL A1688)	
FCC ID: BCG-E2946A)	
IC: 579C-E2946A)	
)	
CURRENTLY LOCATED AT)	
Fairfax County Police Department)	
Organized Crime and Narcotics Section)	

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the search warrant, the application for search warrant, the affidavit in support of the search warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having considered the government's submissions, including the facts presented to justify sealing; having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that, the search warrant, application for search warrant, affidavit in support of the search warrant, Motion to Seal, and this Order be sealed until further Order of the Court.

Date: 23 Aug 17
Alexandria, Virginia

I D D /s/ _____
Ivan D. Davis
United States Magistrate Judge